

REMARKS

The present remarks are in response to the Office Action dated August 20, 2009, in which the Examiner issued a rejection of claims 1-24. The Applicant has amended claims 6, 7 and 9 to remove alternative expressions, cancelled claims 17-24, and added new claims 25-32. In view of the claim amendments and remarks, the Applicant respectfully requests that the pending claims be placed in a state of allowance. No new matter has been added.

A. Claim Amendments

Claims 6, 7 and 9 have been amended to remove alternative expressions using "or." The purpose of this change is to eliminate ambiguity from the claims.

B. New Claims

The new claims are directed to a digital contents illegal use prevention system for distributing a content file. The digital contents illegal use prevention system includes a recording medium distribution device, a recording medium, a management center, a digital contents reproduction device and a communications line.

The recording medium distribution device, shown at 140 in Figure 1, is configured to receive the content file. See Paragraph [0099] (The content file is read out from the master disk set by input section 141 of the recording medium distribution device 140). The content file includes a header and a data body. See Paragraph [0067]. The data body comprises a remaining content file and a piece data file that includes an omitted data file. See Paragraph [0099] (Part of the data body contained in the contents file is separated, and the relevant separated omitted data is recorded on the piece data memory as the piece data).

The recording medium receives the header and the remaining content file associated with the data body. See Paragraph [0099] (After the contents file is separated, the relevant contents file is recorded on the recording medium, e.g., a DVD).

The management center has a database that receives the piece data that includes the omitted data file. See Paragraph [0099] (The piece data is transferred to the management center). The management center is configured to identify an authentic user. See Paragraph [0083] (The management center confirms the authentication of the user).

The digital contents reproduction device is configured to reproduce the content file. See Paragraph [0100] (a digital contents reproducing device is used at least in reproducing the contents file on the recording medium). The digital contents reproduction device includes a reproduction software module configured to read the recording medium for distribution. See Paragraph [0072] and Figure 1 (The digital contents reproducing device 120 includes a reproduction and copy section 124 for reading/writing the data with respect to the recording medium for distribution).

The communications line is configured to support communications between the management center and the digital contents reproduction device. See Paragraph [0066] and Figure 1 (The communication line beta is used to perform intercommunication between the management center 110 and the digital contents reproducing device 120). The management center is configured to communicate the piece data to the digital contents reproduction device after the identity of the authentic user has been confirmed. See Paragraph [0085] and Figure 1 (In the case where it has been confirmed that the user relating to the application is an authentic user, the piece data database 111 is searched to read out the decryption key and the piece data corresponding to the relevant contents ID, and to transmit them to the digital contents reproducing device).

In one embodiment, the piece data file further comprises a location for the omitted data and the management center database is configured to store the location of the omitted data. See Paragraph [0099] (The relevant separated omitted data is recorded on the piece data memory as the piece data together with its location information. The piece data can be sent to the management center). Also see Paragraph [0108] (The piece data consists of omitted data and location information indicating in which part of the data body the relevant omitted data is located).

In another embodiment, the digital contents reproduction device is a general purpose computer. See Paragraph [0072] (The digital contents reproducing device is a general-purpose computer used by the user).

In yet another embodiment, the reproduction software module is downloaded from the management center. See Paragraph [0073] (The reproduction software is downloaded through the communication line from the management center).

In still another embodiment, the data body is encrypted. See Paragraph [0101] (In the recording medium for distribution, the header information and the data body are encrypted).

In a further embodiment, the management center is further configured to collect a charge from a user. See Paragraph [0086] and Figure 1 (The chargers are summed up based on the user information DB and charged to a bank/credit card company 130 or directly to a user).

In a further embodiment, the management center is further configured to send information indicating a rental period to the digital contents reproduction device. See Paragraph [0085] (Where it has been confirmed that the user is an authentic user, the piece data is transmitted to the digital contents reproducing device together with the rental information indicating the rental period).

In a further embodiment, the management center is further configured to transmit a rejection of an application of a user if the user is not confirmed as an authentic user. See Paragraph [0084] (In the case where management center has confirmed that the user relating to the application is an unauthenticated user, the rejection of the application of the user is transmitted to the digital contents reproducing device).

C. Obviousness Rejection (35 U.S.C. § 103)

The Examiner has rejected claims 1-24 under 35 U.S.C. §103(a) as being unpatentable over US Patent No. 7,218,738 to Pedlow, Jr. et al., hereinafter referred to as "Pedlow." The Applicant respectfully disagrees.

Pedlow is directed to selecting portions of content to be encrypted to allow the content to be effectively encrypted for use under multiple decryption systems without

the necessity of encryption of the entire selection of content. See Column 1, lines 52-62 and Column 3, lines 52-67 of Pedlow. In contrast, the Application teaches that a recording medium distribution device receives a content file which includes a header and a data body comprising a remaining content file and a piece data file that includes an omitted data file. The data body of the content may be encrypted in some embodiments. The recording medium, such as a DVD, receives the header and the remaining content, but lacks the omitted data. The omitted data (and in some embodiments, the location of the omitted data), is stored on a management center, such as a server. The digital contents reproduction device, such as a DVD player or a general purpose computer, must communicate with the management center to obtain the omitted data in order to reproduce the content. As indicated in claim 1, omitting the data may produce a bit length different from a decryption bit length, such that decryption fails unless the omitted data has been replaced. The omission of data allows the content owner to control access to content stored on a recording medium in a user's possession.

MPEP § 2143 states that "[t]he key to supporting any rejection under 35 U.S.C. 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious. In this case, the Examiner acknowledges that Pedlow fails to disclose all of the limitations of the claims in the Application. In support of the obviousness rejection, Examiner merely states that, "it would have been obvious to one having ordinary skill in the art to apply partial encryption to omit certain data from encryption because it increased enhanced security making encryption process more complicated and unpredictable."

According to MPEP § 2143, rationales that may support a conclusion of obviousness include:

- (A) Combining prior art elements according to known methods to yield predictable results;
- (B) Simple substitution of one known element for another to obtain predictable results;
- (C) Use of known technique to improve similar devices (methods, or products) in the same way;

- (D) Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results;
- (E) "Obvious to try" - choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success;
- (F) Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations are predictable to one of ordinary skill in the art;
- (G) Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

The Applicant respectfully submits that the Examiner has not articulated the reasons why the invention claimed in the Application is obvious. Examiner bases the assertion of obviousness on a rationale that "it increased enhanced security making encryption process more complicated and unpredictable." This simply restates Examiner's (incorrect) interpretation of the claimed invention, without providing a rationale for why it would have been obvious.

The Examiner's interpretation that the Application teaches "apply[ing] partial encryption" is incorrect. In contrast to the teachings of Pedlow, the Application makes no reference to partial encryption. Pedlow teaches that selected portions of a particular selection of digital content are encrypted while other portions of the content are left unencrypted. See Column 1, lines 53-56. The Application does not teach that portions of the content are left unencrypted. Rather, the invention teaches that a content file includes a header and a data body comprising a remaining content file and a piece data file that includes an omitted data file. Thus, the Application teaches that a portion of the content is omitted on the recording medium from distribution (such as a DVD). The data body may be encrypted, as taught in independent claim 1 and in dependent claim 29, however, in some embodiments the data body is not encrypted. For example, independent claim 25 does not require encryption. See Paragraph [0141] of the Application (it is arbitrary whether or not the encryption is performed).

Furthermore, the Examiner is incorrect that the Application teaches a "more complicated and unpredictable" encryption process. The Application is concerned

with increasing security through the omission of a part of the content data after encryption rather than increasing security through the encryption process itself. Rather than teaching an unpredictable encryption process, the Application teaches that the encryption process used is "well-known." See Paragraph [0183] of the Application.

C. Conclusion

In view of the foregoing, Applicant respectfully argues that claims 1-16 and 25-32 overcome the Examiner's objections and rejections herein and are now patentably distinct and in condition for allowance, which action is respectfully requested.

Respectfully Submitted;

Dated: 2/19/2010

MAK
Michael A. Kerr
Reg. No. 42,722

Michael A. Kerr
Kerr IP Group, LLC
9490 Gateway Drive, Suite 104
Reno, NV 89521
Tel: (775) 624-8700
Fax: (775) 622-0686